

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

BRIAN HUDDLESTON,

Plaintiff,

v.

FEDERAL BUREAU OF
INVESTIGATION and UNITED
STATES DEPARTMENT OF JUSTICE,

Defendants.

CIVIL ACTION No. 4:20CV00447

SEVENTH DECLARATION OF MICHAEL G. SEIDEL

I, Michael G. Seidel, declare as follows:

1. I am the Section Chief of the Record/Information Dissemination Section (RIDS), Information Management Division (IMD), Federal Bureau of Investigation (FBI), Winchester, Virginia. My previous declarations in this matter describe my employment history, responsibilities at the FBI, as well as the FBI's processing of the Freedom of Information Act (FOIA) requests at issue in this case. This is my seventh declaration overall in this instant action and it supplements and incorporates by reference the information previously provided by me in my prior declarations dated December 8, 2020 (First Seidel), dated January 6, 2021 (Second Seidel), dated April 20, 2021 (Third Seidel), dated December 15, 2021 (Fourth Seidel), dated April 29, 2022 (Fifth Declaration), and dated December 9, 2022 (Sixth Declaration). (ECF Nos. 10-1, 12-1, 23-1, 39-1, 54-1, and 84-1.)

2. The FBI submits this declaration in further support of Defendants' Motion for Summary Judgment and to provide the Court with a brief supplemental administrative history of Plaintiff's requests, the procedures used to search for, review and process the additional

responsive records; and, in accordance with *Vaughn v. Rosen*, 424 F. 2d 820 (D.C. Cir. 1973), provide the FBI's justification for withholding information in part or in full pursuant to FOIA Exemptions 1, 3, 4, 6, 7(C), and 7(E), 5 U.S.C. § 552 (b)(1), (b)(3), (b)(4), (b)(6), (b)(7)(C), and (b)(7)(E).

3. In response to Plaintiff's request the FBI processed an additional 205 pages of responsive records subject to the FOIA. Of the 205 pages processed, the FBI released 4 pages in part and withheld 201 pages in full pursuant to applicable FOIA Exemptions or as duplicates to material reviewed and processed elsewhere in the productions provided to Plaintiff.

4. Part I of this declaration provides a supplemental administrative history of Plaintiff's Request to the FBI; Part II provides information concerning the FBI's *Glomar* response relative to Item 4 of Plaintiff's April 9, 2020 FOIA Request; Part III describes the additional searches conducted by the FBI; Part IV describes the FBI's justifications for withholding information in the additional responsive records; and Part V describes the FBI's justification for its standard position to neither confirm nor deny the existence of records within the following categories: national security or foreign intelligence records pursuant to FOIA Exemptions 1 and 3, any individual's name on a watch list pursuant to FOIA Exemption 7(E), records which could identify any participant in the Witness Security Program pursuant to FOIA Exemption 3, records which could reasonably be expected to endanger the life or physical safety of any incarcerated individual pursuant to FOIA Exemptions 7(E) and 7(F), and Confidential Informant Records pursuant to FOIA Exemption 7(D), 7(E) and 7(F).

PART I: SUPPLEMENTAL ADMINISTRATIVE HISTORY OF PLAINTIFF'S REQUESTS

5. The administrative history related to the initial handling of Plaintiff's FOIA requests has been previously discussed in the FBI's Fourth and Sixth declarations in this case.

(ECF Nos. 39-1 and 84-1, Fourth Declaration of Michael G. Seidel, ¶¶ 7-29 and Sixth Declaration of Michael G. Seidel, ¶¶ 3-4.) The subsequent administrative history is outlined below.

6. By letter dated May 23, 2022, the FBI made a fifth release of records to Plaintiff in response to Item number 4 of Plaintiff's request dated April 9, 2020. The FBI advised Plaintiff it reviewed 205 pages and released 4 pages in part, with certain information withheld pursuant to FOIA Exemptions (b)(1), (b)(3), (b)(4), (b)(6), (b)(7)(C), and (b)(7)(E). The FBI further advised Plaintiff he could appeal the FBI's response to OIP within ninety (90) days of its letter. Alternatively, Plaintiff could contact the FBI's public liaison or seek dispute resolution services from OGIS. In addition, the FBI advised Plaintiff that: (i) the records are Bates-numbered FBI(20-cv-447)-1597 through FBI(20-cv-447)-1801; (ii) duplicate copies of the same document were not processed; and (iii) to the extent you seek "any reports from CrowdStrike, Inc. that were obtained by the FBI while assisting Special Counsel Robert Mueller's investigation," FOIA Exemption (b)(7)(E) protects "records or information compiled for law enforcement purposes when disclosure would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law." How the FBI applies its investigative resources against a particular allegation, report of criminal activity, or perceived threat is, itself a law enforcement technique or procedure that the FBI protects pursuant to Exemption (b)(7)(E) of 5 U.S.C. § 552. Accordingly, a confirmation by the FBI that it has or does not have responsive records would be tantamount to acknowledging where the FBI is or is not applying investigative resources thus disclosing the scope of law enforcement techniques and procedures. Other than those processed in this release, the FBI neither confirms

nor denies the existence of additional records pursuant to FOIA Exemption (b)(7)(E) of 5 U.S.C. § 552. (Ex. A.)

PART II: *GLOMAR* RESPONSE – ITEM 4 OF PLAINTIFF’S APRIL 9, 2020 FOIA REQUEST

7. The FBI relies on a *Glomar* response in instances which, assuming that responsive records existed, even acknowledging their existence would result in harms protected against by one or more FOIA exemptions.¹ To be credible and effective, the FBI must use a *Glomar* response in all similar cases regardless of whether responsive records actually exist, including instances in which the FBI does not possess records responsive to a particular request. If the FBI were to issue a *Glomar* response only when it actually possessed responsive records, the *Glomar* response would be interpreted as an admission that responsive records exist.

8. The FBI has determined that merely acknowledging the existence or non-existence of records responsive to Plaintiff’s request for “[a]ny reports from CrowdStrike, Inc. that were obtained by the FBI while assisting Special Counsel Robert Mueller’s Investigation,” would trigger harm under FOIA Exemption (b)(7)(E).

9. Pursuant to FOIA Exemption (b)(7)(E) the FBI does not release information about records or information compiled for law enforcement purposes when disclosure would disclose techniques and procedures for law enforcement investigations or prosecutions or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. The FBI also refuses to confirm or deny the

¹ The phrase “*Glomar* response” stems from a case in which a FOIA requester sought information concerning a ship named the *Hughes Glomar Explorer*, and the CIA refused to confirm or deny its relationship with the *Glomar* vessel because to do so would compromise the national security or divulge intelligence sources and methods. *Phillipi v. CIA*, 655 F.2d 1325 (D.C. Cir. 1981). *Glomar* responses are proper “if the fact of the existence or nonexistence of agency records falls within a FOIA exemption.” *Wolf v. C.I.A.*, 473 F.3d 370, 374 (D.C. Cir. 2007).

existence of responsive records when doing so could provide these types of information.

(b)(7)(E) Glomar

10. FOIA Exemption (b)(7)(E) exempts from disclosure “records or information compiled for law enforcement purposes [when disclosure] would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.” 5 U.S.C. § 552(b)(7)(E). This exemption affords categorical protection to techniques and procedures used in law enforcement investigations; it provides techniques and procedures that are not well-known to the public as well as non-public details about the use of well-known techniques and procedures.

11. How, from whom, and under what circumstances the FBI collects information -- is itself a law enforcement technique or procedure that the FBI protects pursuant to Exemption (b)(7)(E). Thus, the FBI confirming that it has or does not have responsive records would be tantamount to acknowledging where the FBI is or is not applying investigative resources thus disclosing the scope of law enforcement techniques and procedures. Therefore, merely acknowledging the existence or non-existence of records responsive to Plaintiff’s request would trigger harm under FOIA Exemptions (b)(7)(E) with respect to “[a]ny reports from CrowdStrike, Inc. that were obtained by the FBI while assisting Special Counsel Robert Mueller’s Investigation.”

Partial Piercing of (b)(7)(E) Glomar

12. While addressing Item 4 of Plaintiff’s April 9, 2020 FOIA request, the FBI located official, public acknowledgments concerning three (3) CrowdStrike reports in the following documents:

- a. House Permanent Select Committee on Intelligence (HPSCI) – Report on

Russian Active Measures (March 22, 2008).² Within the 253 page HPSCI report on numbered page 36 (.pdf page 46), in Numbers 13-15 it states: “13. HPSCI, Full Committee Briefing on Russia Cyber Activity (Closed Session), Sept. 6, 2016; HPSCI, Full Committee Briefing on Russia Cyber Activity (Closed Session), Jan. 10, 2016; HPSCI, Full Committee Briefing on Russia Cyber Activity (Closed Session), Dec. 5, 2016; [Redaction], *Draft Incident Investigation Report for the Democratic National Committee*” Aug. 24, 2016; [Redaction], *Draft Incident Investigation Report for the Democratic Congressional Campaign Committee*; Aug. 8, 2016.” “14. [Redaction], *Draft Incident Investigation Report for the Democratic National Committee*” Aug. 24, 2016; [Redaction], *Draft Incident Investigation Report for the Democratic Congressional Campaign Committee*; Aug. 8, 2016.” “15. [Redaction], *Draft Incident Investigation Report for the Democratic National Committee*” Aug. 24, 2016; [Redaction], *Draft Incident Investigation Report for the Democratic Congressional Campaign Committee*; Aug. 8, 2016.; LexisNexis, *Discovery Services Fact Sheet: “How Many Pages in a Gigabyte?”* Dec. 23, 2017.”

- b. Unclassified “Report of the Select Committee on Intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election Volume 5: Counterintelligence Threats and Vulnerabilities”.³ Within the 966 page report on numbered page 181 (.pdf page 195), the first paragraph states, among other things, that: “The GRU then established its presence on the DCCC network on April 12, 2016, when hackers leveraged stolen credentials from the compromised DCCC employee to access the DCCC network.” This sentence references Footnote 1170 which states: “(U) *Ibid.*, ¶ 24; CrowdStrike, *Draft Incident Investigation Report, DCCC*, August 8, 2016 (hereinafter *CrowdStrike DCCC Report*), p.6.)”
- c. Doc. 123 dated 05/31/2019 titled “Government’s Response to Defendant’s Motion to Compel Unredacted CrowdStrike Reports” filed in *USA v. Roger J. Stone, Jr.*, Criminal Action No. 1:19-cr-00018-ABJ.⁴ On numbered page 1, in the paragraph beneath the sub-heading “Factual Background”, it states: By May 2016, the Democratic National Committee (“DNC”) and the Democratic Congressional Campaign Committee (“DCCC”) became aware their computer systems had been compromised by intrusions, and they hired the cybersecurity company CrowdStrike to identify the extent of the intrusions and mitigate the

² See https://republicans-intelligence.house.gov/uploadedfiles/final_russia_investigation_report.pdf (Last accessed December 30, 2022.)

³ See https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf (Last accessed December 30, 2022)

⁴ See *United States of America v. Roger J. Stone, Jr.*, Criminal Action Number 1:19-cr-00018-ABJ, Document 123, Filed 05/30/19.

threat. On June 14, 2016, the DNC, via CrowdStrike, publicly announced that it had been hacked by Russian government actors. See, Washington Post, D.N.C. Says Russian Hackers Penetrated its Files, Including Dossier on Donald Trump, June 14, 2016, available at <https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html>. At the direction of the DNC and DCCC's legal counsel, CrowdStrike prepared three draft reports.¹ Copies of these reports were subsequently produced voluntarily to the government by counsel for the DNC and DCCC.²

¹ Although the reports produced to the defendant are marked "draft," counsel for DNC and DCCC informed the government that they are the last version of the report produced.

² The defendant describes the reports as "heavily redacted documents," Doc. 103, at 1. One report is thirty-one pages; only five lines in the executive summary are redacted. Another runs sixty-two pages, and redactions appear on twelve pages. The last report is fifty-four pages, and redactions appear on ten pages.

13. Taking into consideration these public acknowledgments, which partially pierced the FBI's 7(E) *Glomar* veil, FBI-RIDS conducted a search for the three (3) reports responsive to the Plaintiff's request and provided responsive records to Plaintiff in its May 23, 2022 release. Details concerning the FBI's search for records responsive to Item 4 of Plaintiff's April 9, 2020 request is more fully described *infra* ¶ 14 and details concerning the FBI's May 23, 2022 release is more fully described *supra* ¶ 6.

PART III: FBI'S ADDITIONAL SEARCHES

A. SEARCHES CONDUCTED TO LOCATE RECORDS RESPONSIVE TO ITEM 4 OF PLAINTIFF'S APRIL 9, 2020 REQUEST

14. The FBI on March 25, 2022 conducted its initial search for records responsive to Item 4 of Plaintiff's April 9, 2020 request concerning "[a]ny reports from CrowdStrike, Inc. that were obtained by the FBI while assisting Special Counsel Robert Mueller's Investigation." Specifically, the FBI conducted a term search using the term "CrowdStrike" within the SCO investigative files. This search located the three (3) publicly acknowledged reports included in

the production to Plaintiff on May 23, 2022.

B. SEARCHES CONDUCTED TO LOCATE RECORDS RESPONSIVE TO FOIPA NO. 1465531-000; SUBJECT: SETH RICH (JANUARY 1, 2016 TO PRESENT)

15. As discussed in ¶¶ 22-23 of my Fifth Seidel Declaration, Plaintiff contends that there may be other databases that were excluded from the FBI's search. Consistent with FOIA, RIDS search policy is grounded on the principle of reasonableness, not mere possibility. Given the nature of Plaintiff's request (subject reasonably expected to be indexed within the automated indices available in Sentinel or located via a targeted search), the comprehensive nature of the information contained in the Central Records System (CRS), and the subject matter expertise of FBI personnel who conducted targeted searches of records in targeted locations, the FBI conducted searches for responsive records where they could reasonably be expected to be found. As applicable here, Plaintiff provided no information for RIDS to reasonably conclude records would reside in other databases.

16. Nonetheless, in consideration of Plaintiff's concerns, the FBI took the extraordinary step of conducting additional targeted searches within the FBI's Counterintelligence Division (CD)⁵ and its Operational Technology Division (OTD)⁶, to include among others, OTD's Data Intercept Technology Unit. Specifically, using the search terms "Seth Conrad Rich", "Seth C. Rich" and "Seth Rich". These searches yielded no additional records — *i.e.*, no records beyond those contained in the FBI's earlier productions — that are responsive to

⁵ The Counterintelligence Division is a component of the National Security Branch charged with preventing and investigating foreign intelligence activities within the United States. The Counterintelligence Division targets both traditional and emerging nontraditional threats and investigates espionage activities using both intelligence and law enforcement techniques.

⁶ OTD provides technical expertise, services, policy guidance and support to the FBI in collecting evidence and intelligence through the use of lawfully authorized electronic surveillance. OTD's core functions include wireline, wireless, and data network communication technology.

Plaintiff's FOIA request.

PART IV: JUSTIFICATION FOR NONDISCLOSURE UNDER THE FOIA

17. The FBI processed all records responsive to Plaintiff's request to achieve maximum disclosure consistent with the access provisions of the FOIA. Every effort was made to provide Plaintiff with all information in the public domain and with all reasonably segregable, non-exempt information. The FBI did not withhold any reasonably segregable, nonexempt portions from Plaintiff. Further description of the information withheld, beyond what is provided in this declaration, could identify the actual exempt information.

18. Bates Numbering: The FBI numbered all pages of its supplemental production consecutively as FBI(20-cv-447)-1597 through FBI(20-cv-447)-1801.⁷ On the pages released in part, these numbers are typically located at the bottom of each page. Additionally, the FBI is including a *Vaughn* Index at Exhibit B to explain where within its May 23, 2022 production of additional responsive records it withheld pages in their entirety and its reasoning for doing so; and indicate on which pages it asserted various FOIA exemptions.⁸

19. Justification Codes: On the Bates-numbered pages released in part and withheld in full, the FBI further categorized its application of exemptions to better explain the nature of the information withheld pursuant to the provisions of the FOIA. Specifically, the FBI applied numerical codes that coincide with specific categories of exempt information. This declaration

⁷ If requested, the FBI can provide copies of all records processed to the Court for *in camera* inspection.

⁸ In addition, The FBI is including a *Vaughn* Index at Exhibit C to explain where within its December 9, 2022 production of additional responsive records it withheld pages in their entirety and its reasoning for doing so; and to explain on which pages it asserted various FOIA exemptions. Information concerning the FBI's December 9, 2022 production, to include justifications for withholding Bates-numbered pages FBI(20-cv-447)-1803 through 1808 is more fully discussed in my Sixth Declaration. (ECF 84-1 at ¶¶ 4, 15-34.)

and index demonstrate that all information withheld by the FBI is exempt from disclosure pursuant to the cited FOIA exemptions or is so intertwined with non-exempt information that segregation is not possible without revealing the underlying exempt information.

20. Each instance of information withheld pursuant to a FOIA exemption is accompanied by a coded designation that corresponds to one of the categories listed below. For example, if “(b)(7)(C)-1” appears on a page, the “(b)(7)(C)” designation refers to FOIA Exemption 7(C) protecting against unwarranted invasions of personal privacy. The numerical designation “1” following “(b)(7)(C)” narrows the main category into a more specific subcategory, such as “Names and Other Identifying Information of FBI Special Agents and Professional Staff.”

SUMMARY OF EXEMPTION JUSTIFICATION CATEGORIES	
CODED CATEGORIES	INFORMATION WITHHELD
Exemption 1	INFORMATION CLASSIFIED PER EXECUTIVE ORDER 13526
(b)(1)-1	Information currently classified pursuant to Executive Order ("E.O.") 13,526
Exemption 3	Information Protected By Statute
(b)(3)-1	National Security Act of 1947 [50 U.S.C. 3024(i)(1)]
(b)(3)-4	Information Specifically Exempted by Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1504(d)(3)
Exemption 4	Confidential Commercial Information
(b)(4)-1	Confidential Commercial Information
Exemptions (6) & 7(C)	Unwarranted/Clearly Unwarranted Invasion Of Personal Privacy
(b)(6)-1 and (b)(7)(C)-1	Names and Other Identifying Information of FBI Special Agents and Professional Staff
(b)(6)-2 and (b)(7)(C)-2	Names and Other Identifying Information of Third Parties Merely Mentioned
(b)(6)-3 and (b)(7)(C)-3	Names and Other Identifying Information of Persons of Investigative Interest
(b)(6)-7 and (b)(7)(C)-7	Names and Other Identifying Information of Third Party Victims
Exemption 7(E)	Law Enforcement Techniques And Procedures

(b)(7)(E)-1	FBI Internal Email Addresses, Telephone Numbers and Non-Public Web Addresses ⁹
(b)(7)(E)-2	Sensitive Investigative File Numbers and Sub-File Names
(b)(7)(E)-4	Code Names of Investigations
(b)(7)(E)-6	Collection and Analysis of Information
(b)(7)(E)-9	Identities of an FBI Unit, Squad and Division

21. I hereby incorporate by reference the information contained in my Fourth Seidel Declaration concerning FOIA Exemptions (b)(1), (b)(3), (b)(4), (b)(6) and (b)(7)(E),¹⁰ to include specifically, FOIA Exemption Coded Categories (b)(1)-1, (b)(3)-1, (b)(4)-1, (b)(6)-1, 2, 3; (b)(7)(C)-1, 2, 3; and (b)(7)(E)-1, 2, 4, 6, 9 discussed in ¶¶ 86-90, 95-98, 126-131, 158-159, 168, 171 and 176-177. Each of these FOIA Exemption Coded Categories have also been asserted to withhold information in the newly produced records.

22. In addition, to the above mentioned FOIA exemptions and coded categories, the FBI hereby asserts FOIA Exemption 3 to protect information pursuant to the Cybersecurity Information Sharing Act of 2015 (CISA 2015), 6 U.S.C. § 1504(d)(3); Exemptions 6 and 7(C) to protect names and other identifying information¹¹ regarding third party victims and Exemption 7(E) to protect an internal non-public telephone number assigned to and utilized by an FBI Special Agent.

EXEMPTION 7 THRESHHOLD

23. Before an agency can invoke any of the harms enumerated in Exemption (b)(7), it must demonstrate the records or information at issue was compiled for law enforcement

⁹ The FBI is also including in Category (b)(7)(E)-1 Internal, Non-Public Telephone Numbers.

¹⁰ See Fourth Seidel Declaration ¶¶ 76-103, 123-140, and 156-177.

¹¹ *Hereafter*, identifying information includes, but is not limited to, usernames, IP addresses, host names, account names, network addresses, passwords, and security I.D.'s.

purposes. Pursuant to 28 U.S.C. §§ 533 and 534, Executive Order 12333 as implemented by the Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM), and 28 C.F.R. § 0.85, the FBI is the primary investigative agency of the federal government with authority and responsibility to investigate all violations of federal law not exclusively assigned to another agency, to conduct investigations and activities to protect the United States and its people from terrorism and threats to the national security, and to further the foreign intelligence objectives of the United States. Under this investigative authority, the responsive records herein were created and compiled in furtherance of the FBI's role in the Special Counsel's Office (SCO) investigation and related investigations. These records were created and compiled to document the FBI's investigation of potential crimes and threats to the national security, thus, the FBI determined they were created and compiled for law enforcement purposes.¹²

EXEMPTION (B)(1) – CLASSIFIED INFORMATION

E.O. 13526, § 1.4(c) – INTELLIGENCE ACTIVITIES, SOURCES AND METHODS

24. As discussed in my Fourth Seidel Declaration at ¶ 81, E.O. 13526, § 1.4(c), exempts intelligence activities (including covert action), intelligence sources and methods, and cryptology from disclosure.

25. I hereby reassert the information contained in my Fourth Declaration ¶¶ 86-90 concerning the withholding of file numbers and character and titles of cases pursuant to FOIA Exemption 1. Details identifying the specific type of information being withheld pursuant to FOIA Exemption 1 in the additional records processed in response to Plaintiff's FOIA request is set forth in the paragraphs below. The rationale for the withholding of this information and the

¹² Both DOJ and the FBI are responsible for maintaining portions of the SCO record collection, with FBI retaining the investigative records.

harm that would be caused should this information be released remains the same as contained in my Fourth Declaration and is not being recounted verbatim herein.

FILE NUMBERS¹³

26. Within the additional responsive records, the FBI applied Exemption (b)(1)-1 to withhold classified file numbers assigned to specific intelligence activities. This information is properly classified at the “Secret” level pursuant to E.O. 13526 § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

Character and Title of Cases¹⁴

27. Within the additional responsive documents, the FBI also applied Exemption (b)(1)-1 to withhold classified information concerning the character and title of a case for specific types of intelligence activities directed at specific targets of national security interest. This information is properly classified at the “Secret” level pursuant to E.O. 13526 § 1.4(c), and is exempt from disclosure pursuant to Exemption 1.

EXEMPTION (b)(3) – INFORMATION PROTECTED BY STATUTE

28. As discussed in my Fourth Seidel Declaration at ¶ 94, Exemption (b)(3) exempts from disclosure information which is “specifically exempted from disclosure by statute ... if that statute (A)(i) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue; or (A)(ii) establishes particular criteria from withholding or refers to

¹³ FOIA Exemption Category (b)(1)-1 has been asserted by the FBI to withhold information on Bates-numbered page FBI(20-cv-447)-1739.

¹⁴ FOIA Exemption Category (b)(1)-1 has also been asserted by the FBI to withhold information on Bates-numbered page FBI(20-cv-447)-1739.

particular types of matters to be withheld.”

(b)(3)-1: NATIONAL SECURITY ACT OF 1947, 50 U.S.C. § 3024(i)(1)¹⁵

29. I hereby reassert the information contained in my Fourth Declaration ¶¶ 95-98 concerning FOIA Exemption Category (b)(3)-1 to protect from disclosure information pursuant to Section 102A(i)(1) of the National Security Act of 1947 (NSA), as amended by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). This Exemption Coded Category is also applicable to the newly produced records. Specifically in these records, the FBI is asserting Exemption 3, at times in conjunction with Exemptions 1 and 7(E) to withhold information that would reveal classified intelligence sources and methods protected by Exemption 1. In all instances, the information was also withheld under Exemption 7(E) because unclassified intelligence sources and methods were employed as law enforcement techniques, procedures or guidelines, and thus would qualify as both an intelligence source and method under Exemption 3 and a law enforcement technique under Exemption 7(E). Notably, 50 U.S.C. § 3024(i)(1) protects sources and methods regardless of whether they are classified. *See Sims*, 471 U.S. at 176. Thus, the FBI properly withheld this information pursuant to FOIA Exemption (b)(3), in conjunction with Exemptions 1 and 7(E).

(b)(3)-4: Information Specifically Exempted by Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1504(d)(3)¹⁶

30. In December 2015, Congress enacted the Cybersecurity Act of 2015. Title I of the Cybersecurity Act of 2015, 6 U.S.C. §§ 1500-1510, entitled the Cybersecurity Information Sharing Act of 2015 (CISA 2015) provides increased authority for cybersecurity information

¹⁵ FOIA Exemption category (b)(3)-1 has been asserted by the FBI to withhold information on Bates-numbered page FBI(20-cv-447)-1739.

¹⁶ FOIA Exemption category (b)(3)-4 has been asserted by the FBI to withhold information on Bates-numbered pages FBI(20-cv-447)-1598 through 1658, 1660-1707, and 1709-1738.

sharing between and among the private sector; state, local, tribal, and territorial governments; and the Federal Government.¹⁷ The purpose of the CISA 2015 is to encourage robust sharing of useful cybersecurity information among all types of entities—private, Federal, state, local, territorial, and tribal. At the same time, CISA 2015 balances its authorization to share relevant cybersecurity information with the need to safeguard privacy.

31. CISA 2015 provides that cyber threat indicators or defensive measures shared with the Federal Government under CISA 2015 are exempt from disclosure under the Freedom of Information Act. Pursuant to 6 U.S.C. § 1504(d)(3), a cyber threat indicator¹⁸ or defensive measure¹⁹ shared with the Federal Government under this subchapter shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5 and any state, tribal or local provision of law requiring disclosure of

¹⁷ Section 1503(c)(1) authorizes both the sharing and receipt of cyber threat indicators and defensive measures.

¹⁸ The term “cyber threat indicator” is defined in 6 U.S.C. § 1501(6) as: information that is necessary to describe or identify— (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability; (B) a method of defeating a security control or exploitation of a security vulnerability; (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability; (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability; (E) malicious cyber command and control; (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat; (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or (H) any combination thereof.

¹⁹ The term “defensive measure” is defined in 6 U.S.C. § 1501(7)(A) as: an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. 6 U.S.C. § 1501(7)(B) lists certain measures that are excluded from the definition of “defensive measure.”

information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5 and any state, tribal, or local provision of law requiring disclosure of information or records.

32. The FBI asserted Exemption (b)(3)-4 pursuant to CISA 2015 to protect information on Bates-numbered pages FBI(20-cv-447)-1598 through 1658, 1660-1707, and 1709-1738. The withheld information is located on three CrowdStrike Incident Investigation Reports prepared by CrowdStrike in their investigation into the hacking of the computer networks of the Democratic National Committee. This report contains detailed descriptions of the CrowdStrike's investigation into the computer intrusion incident and includes cyber threat indicators as well as defensive measures.

EXEMPTION (B)(4)-1: CONFIDENTIAL COMMERCIAL INFORMATION²⁰

33. As discussed in my Fourth Seidel Declaration at ¶¶ 102-104, Exemption (b)(4) of the FOIA protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." 5 U.S.C. § 552(b)(4). This exemption is intended to protect the interests of both the government and submitters of information. Its very existence encourages submitters to voluntarily furnish useful confidential commercial or financial information to the government and provides the government with an assurance that required submissions will be reliable. The exemption also affords protection to those submitters who are required to furnish confidential commercial or financial information to the government by safeguarding them from the competitive disadvantages that could result from disclosure.

34. For purposes of Exemption 4, commercial and financial information is considered confidential when it is 1) both customarily and actually treated as private by its owner; and 2)

²⁰ FOIA Exemption Category (b)(4)-1 has been asserted by the FBI to withhold information on Bates-numbered pages FBI(20-cv-447)-1597 through 1738.

provided to the government with an assurance of privacy. In reviewing the records at issue, the FBI located information that originated with a private commercial institution. Specifically, the FBI located three (3) reports, clearly marked as “COPYRIGHT PROPRIETARY AND CONFIDENTIAL – NOT TO BE SHARED WITH THIRD PARTIES” and each page of content contains a marking that reads “Privileged and Confidential - Prepared at the Direction of Counsel.” Thus, the FBI determined this confidential commercial information was provided to the FBI under an assurance of confidentiality, and is exempt pursuant to Exemption 4.

EXEMPTIONS (B)(6) AND (B)(7)(C) – UNWARRANTED INVASION OF PERSONAL PRIVACY

35. Exemption 6 exempts from disclosure “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(6). All information that applies to a particular person falls within the scope of Exemption 6.

36. Exemption 7(C) similarly exempts from disclosure “records or information compiled for law enforcement purposes...[when disclosure] could reasonably be expected to constitute an unwarranted invasion of personal privacy.” 5 U.S.C. § 552(b)(7)(C).²¹

37. I hereby reassert the information contained in my Fourth Declaration ¶¶ 126-129 concerning FOIA Exemption Categories (b)(6)-1, 2, and 3 and (b)(7)(C)-1, 2, and 3. Details identifying the specific type of information being withheld pursuant to FOIA Exemptions (b)(6) and (b)(7)(C) in the additional records processed in response to Plaintiff’s FOIA request is set

²¹ The practice of the FBI is to assert Exemption 6 in conjunction with Exemption 7(C). Although the balancing test for Exemption 6 uses a “would constitute a clearly unwarranted invasion of personal privacy” standard and the test for Exemption 7(C) uses the lower standard of “could reasonably be expected to constitute an unwarranted invasion of personal privacy,” the analysis and balancing required by both exemptions are sufficiently similar to warrant a consolidated discussion. The privacy interests are balanced against the public’s interest in disclosure under both exemptions.

forth in the paragraphs below along with information concerning a new (b)(6) and (b)(7)(C) category, cited as (b)(6)-7 and (b)(7)(C)-7. The rationale for withholding information in Categories 1, 2 and 3 and the harm that would be caused should this information be released remains the same as contained in my Fourth Declaration and is not being recounted verbatim herein.

EXEMPTIONS (B)(6)-1 AND (B)(7)(C)-1: NAMES AND OTHER IDENTIFYING INFORMATION OF FBI SPECIAL AGENTS AND PROFESSIONAL STAFF²²

38. Within the additional responsive documents, the FBI applied Exemption (b)(6)-1 and (b)(7)(C)- to withhold information pertaining to the names of FBI Special Agents.²³

EXEMPTIONS (B)(6)-2 AND (B)(7)(C)-2: NAMES AND OTHER IDENTIFYING INFORMATION OF THIRD PARTIES MERELY MENTIONED²⁴

39. Within the additional responsive documents, the FBI applied Exemption (b)(6)-2 and (b)(7)(C)-2 to withhold information pertaining to name of a third party who was merely mentioned in the additional responsive documents.

EXEMPTIONS (B)(6)-3 AND (B)(7)(C)-3: NAMES AND OTHER IDENTIFYING INFORMATION OF THIRD PARTIES OF INVESTIGATIVE INTEREST²⁵

40. Within the additional responsive documents, the FBI applied Exemption (b)(6)-3

²² FOIA Exemption Categories (b)(6)-1 and (b)(7)(C)-1 has been asserted by the FBI to withhold information on Bates-numbered page FBI(20-cv-447)-1739.

²³ The FBI's standard practice is to release the names of Senior Executive Service ("SES") employees because their positions are public facing in nature and therefore, they have a diminished privacy interest in records pertaining to the performance of official duties. The FBI generally draws the line at the non-SES level (GS-15 level employees and below) and protects those names and identifying information pursuant to FOIA Exemptions (b)(6) and (b)(7)(C).

²⁴ FOIA Exemption Categories (b)(6)-2 and (b)(7)(C)-2 has been asserted by the FBI to withhold information on Bates-numbered page FBI(20-cv-447)-1737.

²⁵ FOIA Exemption Categories (b)(6)-3 and (b)(7)(C)-3 has been asserted by the FBI to withhold information on Bates-numbered pages FBI(20-cv-447)-1612 through 1616, 1621-1630, 1636-1638, 1645, 1668, 1671-1672, 1674-1675, 1680, 1682, 1696-1698, 1711, 1714-1730, and 1737.

and (b)(7)(C)-3 to withhold information pertaining to the names and other identifying information of third parties who were of investigative interest to the FBI.

EXEMPTIONS (B)(6)-7 AND (B)(7)(C)-7: NAMES AND OTHER IDENTIFYING INFORMATION
OF THIRD PARTY VICTIMS²⁶

41. In Exemption categories (b)(6)-7 and (b)(7)(C)-7, the FBI protected the names and identifying information of third party victims. Releasing these individuals' identities and information in the context of these reports would cause unsolicited and unnecessary attention to be focused on these individuals. Such a release could force them to relive emotionally trying events, causing further invasion of their privacy, in excess of the harms they've already been forced to endure. Thus, these victims maintain strong privacy interests in the protection of such personal information. Furthermore, there is no legitimate public interest to be served by releasing the identities or information of these victims because their identities, themselves, would not shed light on the operations and activities of the FBI. The FBI determined disclosure of this information would constitute a clearly unwarranted invasion of these individuals' personal privacy, and consequently withheld this information pursuant to FOIA Exemptions 6 and 7(C).

EXEMPTION (b)(7)(E)

INVESTIGATIVE TECHNIQUES AND PROCEDURES

42. Exemption 7(E) protects "records of information compiled for law enforcement purposes" that would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if

²⁶ FOIA Exemption Categories (b)(6)-7 and (b)(7)(C)-7 has been asserted by the FBI to withhold information on Bates-numbered pages FBI(20-cv-447)-1602 through 1603, 1606-1607, 1611-1639, 1645, 1648, 1653, 1657-1658, 1664, 1667, 1671-1673, 1675-1680, 1683, 1685-1688, 1690, 1692-1694, 1696-1698, 1706-1707, 1711, 1713-1719, 1721-1727, 1729-1731, 1736 and 1738.

such disclosure could reasonably be expected to risk circumvention of the law. 5 U.S.C. § 552(b)(7)(E).

43. I hereby reassert the information contained in my Fourth Declaration ¶¶ 157-162, 168, 171 and 176-177 concerning FOIA Exemption Categories (b)(7)(E)-1, 2, 4, 6, and 9. Details identifying the specific type of information being withheld pursuant to FOIA Exemption (b)(7)(E) in the additional records processed in response to Plaintiff's FOIA request along with information concerning an additional type of information the FBI is withholding in Category (b)(7)(E)-1 is set forth in the paragraphs below. The rationale for withholding information in Categories 2 and 3 and the harm that would be caused should this information be released remains the same as contained in my Fourth Declaration and is not being recounted verbatim herein.

(B)(7)(E)-1: FBI INTERNAL EMAIL ADDRESSES, TELEPHONE NUMBERS
AND NON-PUBLIC WEB ADDRESSES²⁷

44. Within the additional responsive documents, the FBI applied Exemption (b)(7)(E)-1 to protect the internal, non-public telephone number of an FBI employee. Releasing this information would provide criminals with specific targets for attacks on FBI communications through "spoofing" or other illegal means.²⁸ For example, "spoofing" occurs when a criminal disguises a communication from an unknown source to appear as if the

²⁷ FOIA Exemption Category (b)(7)(E)-1 has been asserted by the FBI to withhold information on Bates-numbered page FBI(20-cv-447)-1739.

²⁸ As recently as June 3, 2021, the DOJ Office for Immigration Review (EOIR) announced it was notified of phone calls that spoofed the Office of the Chief Immigration Judge as part of a misinformation campaign. Callers spoofed the Office of the Chief Immigration Judge's main line so that calls would appear to be coming from EOIR on the recipient's caller ID. The caller then posed as EOIR employees and sought personal information from the victims. *See*, <https://www.justice.gov/eoir/pr/eoir-warns-scammers-spoofing-agency-phone-number>. (Last accessed January 6, 2022.)

communication is coming from a known, trusted source. Spoofing occurs with emails, telephone calls, and websites. Criminals often use social engineering techniques to elicit sensitive information from the unsuspecting victim. This can be especially dangerous when criminals spoof numbers of law enforcement agencies to appear as if they are from official law enforcement agencies. Victims of such crimes often feel a higher responsibility to respond to questioning and have an expectation that the information they provide will only be used for official law enforcement purposes. Considering the current cyber-security environment where government data breaches and other hacking attempts on government systems are prevalent, it is likely that the release of this type of information could provide hackers with avenues of exploitation. It is possible they could use social engineering to gain further unauthorized access to FBI systems, view and/or manipulate sensitive investigative data, interfere with the FBI's non-public intranet protocol, and/or hinder the FBI's ability to enforce the law by disrupting the FBI's internal communications and by devaluing public trust. Releasing this information poses substantial risks to the FBI's ability to carry out its mission effectively, could potentially decrease the FBI's effectiveness, and could enable criminals to circumvent the law. Accordingly, the FBI asserted Exemption 7(E) to withhold this information.

(B)(7)(E)-2: SENSITIVE INVESTIGATIVE FILE NUMBERS AND SUB-FILE NAMES²⁹

45. Within the additional responsive documents, the FBI applied Exemption

²⁹ FOIA Exemption Category (b)(7)(E)-2 has been asserted by the FBI to withhold information on Bates-numbered page FBI(20-cv-447)-1739.

(b)(7)(E)-2 to protect a sensitive investigative file number and sub-file name.

(B)(7)(E)-4: CODE NAMES FOR INVESTIGATIONS³⁰

46. Within the additional responsive documents, the FBI applied Exemption (b)(7)(E)-4 to withhold information pertaining to a sensitive code name associated with a sensitive law enforcement and national security investigation, which has not been publicly disclosed.

(B)(7)(E)-6: COLLECTION AND ANALYSIS OF INFORMATION³¹

47. Within the additional responsive documents, the FBI applied Exemption (b)(7)(E)-6 to withhold methods it uses to collect and analyze information it obtains for investigative purposes.

(B)(7)(E)-9: IDENTITIES OF AN FBI UNIT, SQUAD AND DIVISION³²

48. Within the additional responsive documents, the FBI applied Exemption (b)(7)(E)-9 to withhold the identity of an FBI Squad involved in the investigation of third parties maintained in the SCO records responsive to Plaintiff's requests.

SEGREGABILITY

49. As discussed in ¶ 3 *supra*, the FBI identified a total of 205 responsive pages: 4 pages Released in Part ("RIP"), and 201 pages Withheld in Full ("WIF"). Each of these categories is discussed below to further address segregability.

a. Pages RIP. Following its segregability review, RIDS determined 4 pages

³⁰ FOIA Exemption Category (b)(7)(E)-4 has been asserted by the FBI to withhold information on Bates-numbered page FBI(20-cv-447)-1739.

³¹ FOIA Exemption Category (b)(7)(E)-6 has been asserted by the FBI to withhold information on Bates-numbered pages FBI(20-cv-447)-1598 through -1658, 1660-1707, and 1709-1739.

³² FOIA Exemption Category (b)(7)(E)-9 has been asserted by the FBI to withhold information on Bates-numbered page FBI(20-cv-447)-1739.

could be released in part with redactions per the identified FOIA exemptions herein. These pages comprise a mixture of material that could be segregated for release and material that was withheld as release would trigger foreseeable harm to one or more interests protected by the cited FOIA exemptions on these pages.

- b. Pages WIF. Following its segregability review, RIDS determined 201 pages required withholding in their entirety. Of these pages, RIDS withheld 139 pages per one or more FOIA exemptions. RIDS determined that all information on these pages was either fully covered by one or more of the cited FOIA exemptions, or determined that any non-exempt information on these pages was so intertwined with exempt material, no information could be reasonably segregated for release. Any further segregation of this intertwined material would employ finite resources only to produce disjointed words, phrases, or sentences, which taken separately or together, would have minimal or no informational content. The remaining 61 pages were found to be duplicates of other pages accounted for elsewhere within the FBI's production. It is RIDS' policy not to process duplicates as doing so would consume finite FOIPA processing resources to provide the public with no additional net information about FBI actions or operations.

PART V: THE FBI'S STANDARD *GLOMAR* RESPONSES

- 50. The FBI relies on a *Glomar* response to FOIPA requests when acknowledging the existence or non-existence of certain categories of responsive records would result in harm to an

interest protected by one or more FOIA exemptions.³³ To be credible and effective, the FBI must assert a *Glomar* response regardless of whether responsive records exist (*i.e.*, including when the FBI does not possess responsive records). If the FBI invoked a *Glomar* response only when it possesses responsive records, the *Glomar* response would be interpreted as an admission that responsive records exist. This is especially important because the FBI serves dual functions as the country's main internal intelligence agency and a federal law enforcement agency.

51. *Organizations*: To the extent a request for records on organizations may implicate classified or unclassified intelligence records and acknowledging the existence or non-existence of such records would harm an interest protected by the FOIA, a *Glomar* response pursuant to Exemptions 1 and/or 3, in conjunction with the National Security Act of 1947 [5 U.S.C. §§ 552(b)(1), (b)(3) and/or 50 U.S.C. § 3024(i)(1)], as applicable, is asserted.

52. *Justification*: To the extent a request for records implicates unacknowledged records concerning an individual, the FBI also asserts the above *Glomars* pursuant to Exemptions 1 and 3, in conjunction with the National Security Act of 1947 [5 U.S.C. §§ 552(b)(1), (b)(3) and/or 50 U.S.C. § 3024(i)(1)], as applicable. Additionally, the FBI asserts several other *Glomar* responses to requests on individuals. First, pursuant to Exemption 3, in conjunction with 18 U.S.C. § 3521(b)(1)(G), the FBI can neither confirm nor deny the existence of records which could identify a participant in the Witness Security Program. Second, pursuant to Exemption 7(E), the FBI can neither confirm nor deny the existence of an individual's name on a watch list. Third, pursuant to Exemptions 7(E) and 7(F), the FBI can neither confirm nor deny the existence of unacknowledged records or information which could reasonably be expected to endanger the life or physical safety of any incarcerated individual. Finally, pursuant

³³ See Footnote 1 *supra*, describing the phrase "*Glomar* response".

to Exemption 7(D), 7(E), and 7(F), the FBI can neither confirm nor deny the existence of unacknowledged records or information concerning the use of confidential human sources in the context of a specific investigation.

53. As previously noted, to be credible and effective, the FBI must assert a *Glomar* response regardless of whether responsive records exist (*i.e.*, including when the FBI does not possess responsive records). If the FBI invoked a *Glomar* response only when it possesses responsive records, the *Glomar* response would be interpreted as an admission that responsive records exist. The FBI includes an addendum with each response letter which informs the requester of the FBI's standard *Glomar* position as to certain types of records, and further advises that the inclusion of the standard addendum is not an indication that records do or do not exist. Consistent with the process, the FBI incorporates by reference the standard justification for these *Glomar* responses as an exhibit to the FBI's public declaration, whether such records do or do not exist. (Ex. D.)

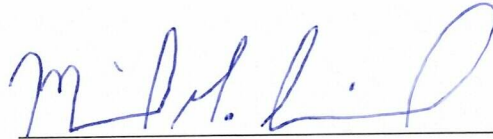
CONCLUSION

54. The FBI performed adequate and reasonable searches for responsive records, processed all such records, and released all reasonably segregable non-exempt information from documents responsive to Plaintiff's FOIA requests that are subject to FOIA. The FBI processed the additional records under the access provisions of the FOIA to achieve maximum disclosure. Information was properly withheld pursuant to FOIA Exemptions 1, 3, 4, 6, 7(C) and 7(E), 5 U.S.C. § 552(b)(1), (b)(3), (b)(4), (b)(6), (b)(7)(C), and (b)(7)(E). The FBI carefully examined the documents and determined the information withheld from Plaintiff in this case, if disclosed, would reveal classified information; would reveal statutorily protected information; would reveal confidential trade secrets and commercial information; would cause a clearly unwarranted invasion of the personal privacy, or could reasonably be expected to constitute an unwarranted

invasion of personal privacy; and would disclose techniques and procedures for law enforcement investigations. After extensive review of these additional documents at issue, the FBI determined that there is no further non-exempt information that can be reasonably segregated and released without revealing exempt information. The FBI also provided Plaintiff with its standard *Glomar* response concerning unacknowledged intelligence records, watch list records, witness security program records, records for incarcerated individuals, and records of confidential human sources advising that it can neither confirm nor deny the existence of such records pursuant to FOIA Exemptions 1, 3, 7(D), 7(E) and 7(F).

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct, and that Exhibits A-D attached hereto are true and correct copies.

Executed this 20th day of January 2023.



MICHAEL G. SEIDEL

Section Chief

Record/Information Dissemination Section

Information Management Division

Federal Bureau of Investigation

Winchester, Virginia